Docket No.: 08226/100S142-US3
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Letters Patent of:
Mark Delany

Patent No.: 7,313,700

Issued: December 25, 2007

For: METHOD AND SYSTEM FOR
AUTHENTICATING A MESSAGE SENDER
USING DOMAIN KEYS

REQUEST FOR CERTIFICATE OF CORRECTION
PURSUANT TO 37 CFR 1.323 AND 1.322

Attention: Certificate of Correction Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Upon reviewing the above-identified patent, Patentee noted typographical errors which should be corrected. A listing of the errors to be corrected is attached.

The typographical errors marked with an "A" on the attached list are found in the application as filed by applicant. Payment in the amount of $100.00 covering the fee set forth in 1.20(a) is enclosed.

The typographical errors marked with a "P" on the attached list are not in the application as filed by applicant. Also given on the attached list are the documents from the file history of the subject patent where the correct data can be found.

The errors now sought to be corrected are inadvertent typographical errors the correction of which does not involve new matter or require reexamination.

Transmitted herewith is a proposed Certificate of Correction effecting such corrections. Patentee respectfully solicits the granting of the requested Certificate of Correction.

The Commissioner is authorized to charge any deficiency of up to $300.00 or credit any excess in this fee to Deposit Account No. 04-0100.

Dated: January 18, 2008

Respectfully submitted,

By_____

Flynn Barrison
Registration No.: 53,970
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770
(212) 527-7700
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant

PTO/SB/44 (04-05)
Approved for use through 04/30/2007. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,313,700 Page 1 of 1

APPLICATION NO.: 10/805,181

ISSUE DATE : December 25, 2007

INVENTOR(S) : Delany

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 7, line 20, delete "Signature: "header" and insert - - Signature:" header - -, therefor.

In column 7, line 27, before "DomainKey-Signature:" insert - - " - -.

In column 7, line 61, delete "19rOUi4" and insert - - 19r0Ui4 - -, therefor.

In column 7, line 61, delete "3NOq" and insert - - 3N0q - -, therefor.

In column 8, line 13, below "Hi." delete ".etc" and insert - - ..etc - -, therefor.

In column 17, line 9, in Claim 18, after "comprising" insert - - : - -.

MAILING ADDRESS OF SENDER (Please do not use customer number below):
John W. Branch, Esq.
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770

1

Darby & Darby

Issued Patent Proofing Form **File#: 08226/100S142-US3**
Note: P = PTO Error **A = Applicant Error**

US Serial No.: 10/805,181 **US Patent No.: US 7,313,700 B2** **Issue Dt.: Dec. 25, 2007**
Title: METHOD AND SYSTEM FOR AUTHENTICATING A MESSAGE SENDER USING DOMAIN KEYS

Sr. No.	P/A	Original		Issued Patent		Description Of Error
		Page	Line	Column	Line	
1	P	Page 12 Specification (03/19/2004)	4	7	20	Delete "Signature: "header" and insert - - Signature:" header - -, therefor.
2	A	Page 12 Specification (03/19/2004)	10	7	27	Before "DomainKey-Signature:" insert - - " - -.
3	P	Page 13 Specification (03/19/2004)	13	7	61	Delete "19rOUi4" and insert - - 19r0Ui4 - -, therefor.
4	P	Page 13 Specification (03/19/2004)	13	7	61	Delete "3NOq" and insert - - 3N0q - -, therefor.
5	P	Page 14 Specification (03/19/2004)	4	8	13	Below "Hi." delete ".etc" and insert - - ..etc - -, therefor.
6	A	Page 5 Claims (06/25/2007)	Claim 18 Line 1	17	9	In Claim 18, after "comprising" insert - - : - -.

(5) If no "from domain" is found, apply the local policy.

(6) Query for the public key component based on the signature type, selector, the "from domain," and the like. In the case of the DNS, the query may be of the form of a TXT record for the name $selector._smtp._domainkey.$fromdomain, or the like.

(7) If the query fails to respond, defer acceptance of this message.

(8) If the query fails because the record does not exist, apply the local policy.

As an interim until widely adopted, the Domain Key application can use a place-holder DNS entry at the _smtp._domainkey.node which indicates whether that particular domain is participating in the Domain Key application or not. The presence of the place-holder indicates participation while the absence of the place-holder indicates non-participation.

(9) Using the public key component returned from the query, check the signature against the entire contents of the email following the "DomainKey-Signature: "header line. Again, the contents are canonically treated in exactly the same way as they are in the signing process.

(10) If the digital signature fails, apply local policy.

(11) In all cases where the message is accepted for delivery, local policy may be conveyed to the message client via a "DomainKey-Status:" header line that precedes the DomainKey-Signature:" header line.

EXAMPLES

The following example for the Domain Key application is intended to introduce at least one embodiment of the present invention and illustrate how its concepts may be integrated into a flow of email.

Email Composed by User

From: "Joe SixPack"<joe@football.example.com>
To: "Suzie Q"<suzie@shopping.example.net>
Subject: Is dinner ready?
Date: Fri, 11 Jul. 2003 21:00:37-0700 (PDT)
Message-ID:
<20030712040037.46341.5F8J@football.example.com>
Hi.
We lost the game. Are you hungry yet?
Joe.

Nothing about the email authorship process is changed by the Domain Key application. In some implementations it is expected that the sender may have no need to know that the Domain Key application exists.

Email Signed by Sending Email Server

Using the private key component, this email is signed by the example.com outbound mail server and now looks something like this:

DomainKey-Signature:
sigs-0.50:D8CD98F00B204E98:
AMLfamjh4GrUzSN5BeUC13qwlq/hL6 GOk8M/
1UNjSRruBNmRugCQoX7/
mfISbSF5Dimr5ey1K6MZg0XclZucPW/s9UWm/
mxqWP 5uD4tB6G+MbSicsj/QohMIBIQjNzRX7A
19xOUt4jNFzjDVtO74vgMlMJepyJR3NOqPm8zGe+g
XhcNBbCuxE0T2keDkJQP8ZJtlWL+
t6lhbTX3vWxtK0CtjaXYCxVJ5loyroMxfpdwUd6d0lfEa
bodyC1Tu+9xvOfHVK+JK7rz+
wwbvRrxiLfrYigYTm4TQ9v1HkW9nt9/7aLw/rN2Fs/
kGwKM ZwxQ9ypgi9qOpNX/TAceElOp8+
jAXW70R7pZYzdrNTq0/1fZu76nq6YnQux7

Received: from dsl-10.2.3.4.network.example.com [10.2.3.4] by submitserver.example.com with SUBMISSION;
Fri, 11 Jul. 2003 21:01:54-0700 (PDT)
From: "Joe SixPack"<joe@football.example.com>
To: "Suzie Q"<suzie@shopping.example.net>
Subject: Is dinner ready?
Date: Fri, 11 Jul. 2003 21:00:37-0700 (PDT)
Message-ID: <20030712040037.46341.5F8J@football.example.com>
Hi.
.etc

Here we can see that additional header lines have been added to this email. Of particular interest are the contents of the "DomainKey-Signature:" line, which has three colon separated components:

(1) A digital signature type and version—in this case "sigs-0.50". This defines which algorithm is used to check the signature. It also defines the location and form of the query used to retrieve the corresponding Public Key.

(2) The Domain Key Selector—in this case "D8CD98F00B204E98". This selector is used to form a query for the Public Key. It is understood that a selector can be provided by which multiple Public Keys for a single domain name might co-exist.

(3) The digital signature data encoded as a base64 string—in this case the string starting with "AMLfamjh4GrUzSN". This is the output of the digital signature generation process.

White spaces are typically ignored in this header and may be removed when using the components to verify the email. The signature typically applies to every line following the first "DomainKey-Signature:" header line.

Note that as some email systems re-write headers, it may be appropriate to sign a canonical form of vulnerable headers and sign a specific subset of header.

Authentication of Email by Receiving Email Server

For an email, the digital signature is normally authenticated by the final delivery agent. However, intervening mail servers may also perform this authentication if they choose to do so.

One embodiment of a process for authentication includes the following steps:

(1) The selector and digital signature are extracted from the "DomainKey-Signature:" header line.

(2) The domain is extracted from the sender address. This is the contents of the first "From:" header. If no domain can be extracted, then extract from the first "Sender:" header line. If no domain can be extracted then the domain is extracted from the envelope sender.

(3) The DNS is queried for a TXT record associated with the following name:

D8CD98F00B204E98._smtp._domainkey.example.com

Note that the selector "D8CD98F00B204E98" forms part of the DNS query as part of the Domain Key process.

(4) The returned TXT record includes the base64, or the like, encoded Public Key for that selector/domain combination. This Public Key may be used to authenticate the digital signature according to the Signature type and version algorithm.

(5) If no TXT record exists, the digital signature is a forgery or this Domain key pair has been revoked by the domain owner.

17. The method of claim 1, wherein employing the policy, further comprises if it is determined that the domain is relatively new to a messaging system, employing a new domain policy for handling an amount of verified digitally signed messages that are less than a predetermined limit over a period of time, wherein each message that is greater than the predetermined limit is handled with at most partial rejection.

18. The method of claim 1, further comprising[]

generating a personal digital certificate for the sender based on the public component and the private component of the key pair associated with the domain;

providing a public component of the personal digital certificate to the recipient along with the verified digitally signed message; and

enabling the recipient to subsequently provide a response message to the sender that is automatically encrypted with the public component of the sender's personal digital certificate.

19. The method of claim 18, wherein the personal digital certificate is associated with an address of the sender.

20. A server for message authentication, comprising:

a memory for storing instructions;

a processor for enabling actions based on the stored instructions, including:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name system (DNS) server that is associated with the domain;

if a message originates from a sender's address associated with the domain, employing a private component of the key pair to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS server verifies that the digitally signed message originated from the domain associated with the sender's address, employing at least one policy associated with the originating domain to handle the verified digitally signed message for the recipient;

else handling the message from another sender's address associated with an unverified domain.

21. The server of claim 20, wherein the at least one policy includes at least one of an unverified domain policy, a verified domain policy, a new domain policy, a system policy, a user policy, a statistics policy, and a third party policy.

22. The server of claim 20, the actions further comprising:

generating a personal digital certificate for the sender based on the public component and the private component of the key pair associated with the domain, wherein the personal digital certificate is associated with an address of the sender;

providing a public component of the personal digital certificate to the recipient along with the verified digitally signed message; and

enabling the recipient to subsequently provide a response message to the sender that is automatically encrypted with the public component of the sender's personal digital certificate.

23. A client for message authentication, comprising:

a memory for storing instructions;

a processor for enabling actions based on the stored instructions, including:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name system (DNS) server that is associated with the domain;

if a message originates from a sender's address associated with the domain, employing a private component of the key pair to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS server verifies that the digitally signed message originated from the domain associated with the sender's address, employing at least one policy associated with the originating domain to handle the verified digitally signed message for the recipient;

else handling the message from another sender's address associated with an unverified domain.

24. The client of claim 23, wherein the at least one policy includes at least one of an unverified domain policy, a verified domain policy, a new domain policy, a system policy, a user policy, a statistics policy, and a third party policy.

25. The client of claim 23, the actions further comprising:

generating a personal digital certificate for the sender based on the public component and the private component of the key pair associated with the domain, wherein the personal digital certificate is associated with an address of the sender;

providing a public component of the personal digital certificate to the recipient along with the verified digitally signed message; and

enabling the recipient to subsequently provide a response message to the sender that is automatically encrypted with the public component of the sender's personal digital certificate.

26. A computer readable storage medium that includes instructions for performing actions, comprising:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name system (DNS) server that is associated with the domain;

if a message originates from a sender's address associated with the domain, employing a private component of the key pair to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS server verifies that the digitally signed message originated from the domain associated with the sender's address, employing at least one policy associated with the originating domain to handle the verified digitally signed message for the recipient;

else handling the message from another sender's address associated with an unverified domain.

27. The computer readable storage medium of claim 26, the actions further comprising:

generating a personal digital certificate for the sender based on the public component and the private component of the key pair associated with the domain, wherein the personal digital certificate is associated with an address of the sender;

providing a public component of the personal digital certificate to the recipient along with the verified digitally signed message; and

enabling the recipient to subsequently provide a response message to the sender that is automatically encrypted with the public component of the sender's personal digital certificate.